Analisis Performa Site to Site IP *Security Virtual Private Network* (VPN) Menggunakan Algoritma Enkripsi ISAKMP

(Performance Analysis Site to Site IP Security Virtual Private Network (VPN) with Algorithm Encryption ISAKMP)

Firmansyah[1], Mochamad Wahyudi[2], Rachmat Adi Purnama[3]

[1]*Sistem Informasi, Sekolah Tinggi Manajemen Informatika dan Komputer Nusa Mandiri Jakarta (STMIK Nusa Mandiri Jakarta)*
Jl. Damai No. 8, Warung Jati Barat (Margasatwa), Pasar Minggu, Jakarta Selatan
[2]*Teknologi Informasi, Universitas Bina Sarana Informatika*
[3]*Teknologi Komputer, Universitas Bina Sarana Informatika*
JL. Kamal Raya No. 18, Cengkareng Barat, Cengkareng, Jakarta Barat

[1]firmansyah.fmy@nusamandiri.ac.id
[2]wahyudi@bsi.ac.id
[3]rachmat.rap@bsi.ac.id

Abstrak – Perkembangan jaringan internet sudah tidak terbendung lagi, hal ini dapat menyebabkan potensi terjadinya ancamanan didalam dunia intenet. Penggunaan Virtual Private Network (VPN) nampaknya menjadi salah satu metode keamanan jaringan yang sangat baik dalam melakukan pendistribusian layanan paket data didalam jaringan internet. Penggunaan VPN mampu memangkas alokasi penggunaan bandwidth serta meminimalisir terjadinya kebocoran terhadap paket data yang sedang ditransfer. Site to Site merupakan salah satu metode VPN IPSec Tunneling yang sering digunakan untuk menghubungkan antara lokasi yang berbeda agar menjadi satu kesatuan network. Penggunaan IPSec dapat melindungi transfer data antara host to host, network to network hingga network to host dikarenakan melakukan pengenkripsi terhadap paket data yang ditransfer. Hasil pengujian dalam pengimplementasian jaringan Site to Site IP Security Virtual Private Network With Algorithm Encryption ISAKMP didapatkan pengurangan hops terhadap jaringan yang menggunakan tunnel dengan Time to Live (TTL)=126 sedangkan jaringan tanpa menggunakan tunnel memiliki nilai TTL sebesar 124.

Kata-kata kunci: VPN, Site to Site, Tunnel VPN, ISAKMP, IP Sec.

Abstract -The development of the internet network has been unstoppable, create oportunities for threats in the internet. The Virtual Private Network (VPN) seems to be one of the excellent network security methods in distributing data packet services in the internet. VPN can reduce the allocation of bandwidth usage and minimize the occurrence of leakage of data packets that are being transferred. Site to Site is IPSec Tunneling VPN methods that used to connect between different locations to become a single network entity. IPSec can protect the transfer of data between host to host, network to network to network to host due to encrypting the packet of data. Test results in network implementation Site to Site IP Security Virtual Private Network With ISAKMP Encryption Algorithm there is a reduction in hops to networks that use tunnels with Time to Live (TTL) = 126 while networks without using tunnels have TTL values of 124

Keywords: VPN, Site to Site, Tunnel VPN, ISAKMP, IP Sec

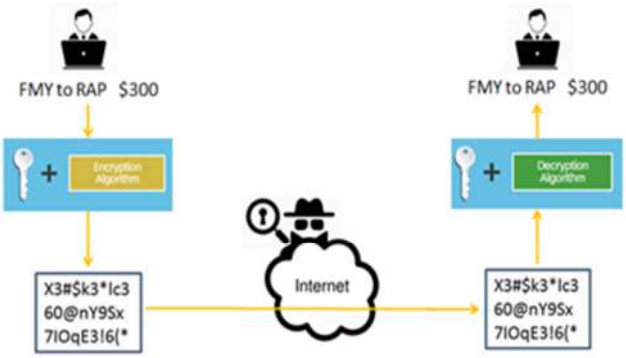
I. PENDAHULUAN

Virtual Private Network (VPN) nampaknya menjadi salah satu metode keamanan jaringan yang sangat baik dalam melakukan pendistribusian layanan paket data didalam jaringan internet. Penggunaan layanan VPN mampu menawarkan konsep penggunaan bandwidth yang efesien, fungsional yang lebih fleksibel dan keamanan yang bersifat privasi [1]. Dengan mengimplementasikan VPN merupakan sebuah langkah awal melindungi paket IP didalam jaringan internet, baik mengamankan situs-situs atau melakukan remote akses dengan jarak yang berjauhan [2].

Dalam jaringan komputer, keamanan paket data sewaktu pengiriman dan penerimaan paket data sangatlah penting untuk menjamin bahwa paket data

yang dikirimkan sampai pada pihak yang dituju, dan tidak jatuh pada pihak yang tidak berkepentingan [3]. Permasalahan terhadap keamanan jaringan selalu dikembangkan sejalan dengan perkembangan teknologi informasi. Penggunaan IP *Security* (IPSec) merupakan sebuah metode enkripsi yang digunakan untuk melindungi kerahasiaan, dan keutuhan data pengguna layanan di jaringan internet [4]. Terlihat pada Gambar 1, bagaimana cara kerja dari penggunaan Enkripsi didalam jaringan komputer. Penerima paket data akan dapat membaca pesan yang dikirimkan oleh pengirim jika mengetahui *key* dari enksripsi yang digunakan.

IPSec merupakan skema keamanan *end to end* yang beroperasi didalam jaringan internet [5]. Penggunaa IPSec dapat melindungi transfer data antara *host to host*, *network to network* atau di antara *network* dengan *host*. Penggunaan IPSec dapat meminimalisir dari serangan *spying* didalam jaringan dikarenakan IPSec melakukan enkripsi terhadap paket data didalam lalu lintas jaringan.

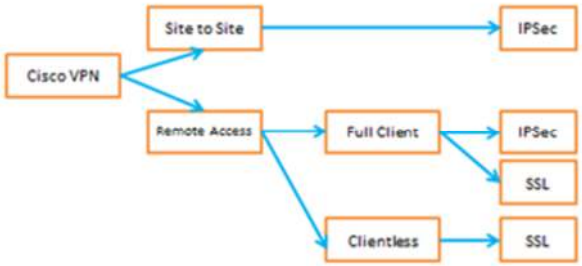


Gambar 1. Konsep enkripsi

Penggunaan VPN dapat menghubungkan dua atau lebih perangkat jaringan melalui jaringan publik menggunakan enkripsi atau dengan menggunakan cara lain untuk mengamankan transmisi antara perangkat jaringan [6]. Dengan menggunakan VPN Tunnel pada jaringan internet, memungkinkan jaringan komputer memiliki jalur yang terpisah secara geografis dan dapat melakukan pemangkasan terhadap hops yang dilalui.

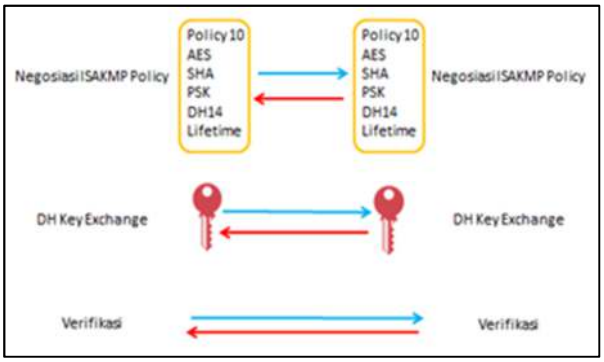
Pada penelitian sebelumnya, jaringan IPSec VPN gateway digunakan untuk menghubungkan jaringan lokal di pusat dengan jaringan lokal di perwakilan, sehingga masing-masing PABX berbasis IP dapat berkomunikasi secara internal [7]. Sedangkan pada penelitian lainnya, IPSec Tunnel tidak menjamin dari serangan *Denial of Service* (DoS), dari pengujian didapat packet loss mencapai kisaran 30 persen yang artinya masih dibawah standar ITU-T G.104 yang memiliki ambang batas maksimal 20 persen [8].

Pengimplementasian protokol IPSec mampu menggabungkan dua mode enkripsi secara bersamaan [9] dengan melakukan enkapsulasi paket data dengan header di kedua ujungnya [10]. Setiap paket data akan dienkapsulasi didalam datagram IP menggunakan alamat IP router melalui tunnel alamat tujuan [11]. Dilihat dari manfaat penggunaannya jaringan VPN mampu, bersifat pribadi dikarenakan VPN menggunakan metode pemisah jalur yang berbeda untuk menjaga tranfer paket data [12]. Pengimpelentasian logika tunnel mampu membawa paket IP address tidak tergantung berdasrkan muatan dan protokol yang digunakan [13]. Terdapat dua tipe dari VPN, yaitu: *Remote Access* VPN dan *Site to Site* VPN *Access*, terlihat pada Gambar 2 yang menjelaskan tipe-tipe dari pembagian cara kerja dari sebuah jaringan VPN.



Gambar 2. Cisco VPN

Penggunaan *site to site* VPN memungkinkan komputer *client* dengan lokasi yang berbeda dapat saling berkomunikasi secara transparan sehingga dapat saling berbagi sumber daya antara lokasi melalui jaringan internet. Dalam pengimplementasiannya, sejumlah tunnel digunakan untuk menghubungkan VPN dari router agar dapat saling berkomunikasi [14]. Setiap sisi *router* yang terhubung dengan VPN *tunnel* dikonfigurasi untuk menentukan rute yang akan dilalui. Untuk mendukung kinerja VPN yang terenkripsi dapat mengunakan metode enkripsi ISAKMP. *Internet Security Association and Key Management Protocol* (ISAKMP) mampu mendefenisikan prosedur dan format dari sebuah paket yang telah ditetapkan, mampu bernegosiasi, memodifikasi dan menghapus *security associations* [15] sebagaimana pada Gambar 3.

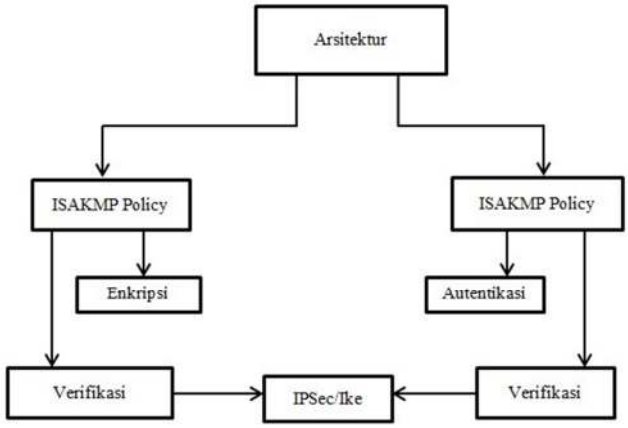


Gambar 3. Kebijakan ISAKMP

ISAKMP dapat bekerja dengan banyak perbedaan protokol keamanan jaringan. Dapat dijelaskan pada Gambar 3 merupakan kebijakan yang dilakukan pada Protokol ISAKMP. ISAKMP melakukan negosiasi kebijakan diantara kedua router yang akan melakukan tunneling. Jika diantara kedua router yang akan melakukan tunneling menggunakan ISAKMP Policy yang sama maka lalu lintas tunneling akan diizinkan.

II. METODE

Dalam melakukan penelitian *site to site ip security virtual private network* (vpn) *with algorithm encryption* isakmp penulis menggunakan bantuan *software* simulasi Cisco Packet Tracer. *Software* ini digunakan untuk membuat simulasi jaringan yang dijalankan secara virtualisasi namun tidak merubah dan mengurangi fitur *device* aslinya. Untuk mengimplementasikan jaringan *site to site ip security virtual private network* penulis mengggunakan bantuan empat (4) buah perangkat *router series* 1941 dengan menggunakan IOS version 15.1 (4) M4 (Gambar 4).



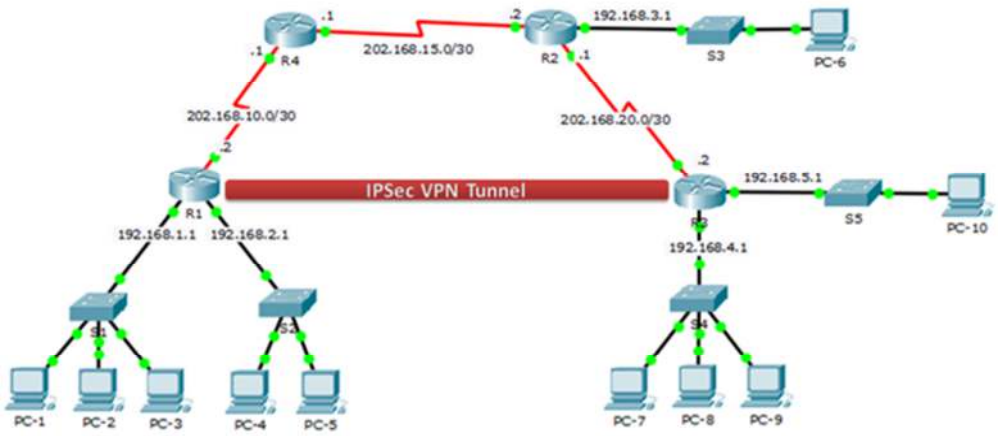
Gambar 4. Metode Penelitian

Terlihat pada Gambar 4 merupakan tahapan metode penelitan yang digunakan dalam penelitan *site to site ip security virtual private network* (vpn) *with algorithm encryption* isakmp. Setiap router yang akan mengimplementasikan IPSec-ISAKMP melakukan pengaktifan *technology-package securityk9* dengan menerapkan keamanan enkripsi aes 256 untuk metode autentikasi dan verifikasi terhadap protokol enkripsi yang digunakan.

III. HASIL DAN PEMBAHASAN

A. *Skenario Simulasi*

Untuk melakukan implementasi jaringan *site to site ip security virtual private network (vpn) with algorithm encryption* isakmp penulis menggunakan skema jaringan yang terlihat pada Gambar 5 dengan spesifikasi IP *Address* yang terlihat pada Tabel 1. Terdapat beberapa skenario pengujian dalam penelitian ini, diantaranya pengujian *hops* yang dilalui untuk melihat cara kerja dari sebuah tunnel didalam jaringan VPN serta melihat pengiriman packet yang terenkripsi.



Gambar 5. Skema jaringan IPSec VPN *tunnel*

Dijelaskan pada Gambar 5, IPSec VPN Tunnel digunakan untuk menghubungkan antara jaringan lokal yang terdapat pada R1 dengan jaringan lokal R3 khususnya pada jaringan lokal yang terhubung dengan S4, dengan metode ini diharapkan dapat meminimalisir jumlah *hops* yang terbentuk antara R1 dengan R3. Jaringan lokal yang terdapat pada R3 dengan menggunakan S5 nantinya tidak didaftarkan ke dalam *Access List* dikarenakan sebagai pembanding antara *network* yang berstatus *permit* dengan *network* yang berstatus *deny* di dalam jaringan *Tunnel*.

TABEL I
SPESIFIKASI IP ADDRESS

Device	Interface	IP Address
R1	G0/0	192.168.1.1/24
	G0/1	192.168.2.1/24
	S0/0/0	202.168.10.2/30
R2	G0/0	192.168.3.1/24
	S0/0/0	202.168.15.2/30
	S0/0/1	202.168.20.1/30
R3	G0/0	192.168.4.1/24
	G0/1	192168.5.1/24
	S0/0/1	202.168.20.2/30
R4	S0/0/0	202.168.10./30
	S0/0/1	202.168.15.1/30

B. Konfigurasi Package Securityk9

Pengaktifan *technology-package securityk9* merupakan dasar dari pengaktifan keamanan terhadap jaringan VPN tunnel. *Package* ini diaktifkan terhadap router yang akan melakukan VPN Tunnel yaitu R1 dan R3. Perintah yang digunakan untuk pengaktifan *Security technology package* menggunakan perintah "R1(config)#license boot module c1900 technology-package securityk3". Setelah melakukan pengaktifkan *package*, lakukan penyimpanan konfigurasi dan *reload* router untuk mengaktifkan lisensi dari securityk9.

```
Technology Package License Information for Module:'c1900'

-----------------------------------------------------------------
Technology    Technology-package          Technology-package
              Current       Type          Next reboot
-----------------------------------------------------------------
ipbase        ipbasek9      Permanent     ipbasek9
security      securityk9    Evaluation    securityk9
data          disable       None          None
```

Gambar 6. Technology-package

Terlihat pada Gambar 6 merupakan database dari technology package pada router cisco yang meliputi: ipbase, security serta data. Jika technology package belum diaktifkan maka akan berstatus *disable* dan *none*.

C. Access List

Access List digunakan untuk memberikan batasan terhadap hak akses didalam jaringan lokal R1 dengan jaringan lokal yang terdapat pada R3 dalam melakukan transfer paket data yang terenkripsi. *Access list* diimplementasikan pada R1 terhadap *network* 192.168.1.0/24 dan 192.168.2.0/24, sedangkan *access list* pada R3 diimplmentasiakan terhadap *network* 192.168.4.0/24.

```
R1(config)#access-list 110 permit ip 192.168.1.0
   0.0.0.255 192.168.4.0 0.0.0.255
R1(config)#access-list 110 permit ip 192.168.2.0
   0.0.0.255 192.168.4.0 0.0.0.255

R3(config)#access-list 110 permit ip 192.168.4.0
   0.0.0.255 192.168.1.0 0.0.0.255
R3(config)#access-list 110 permit ip 192.168.4.0
   0.0.0.255 192.168.2.0 0.0.0.255
```

Penggunaan *access list* pada jaringan Tunnel VPN dapat menentukan *network* mana sajakah yang berstatus *permit* maupun *deny*, serta dapat melakukan isolasi terhadap lalu lintas data di dalam jaringan.

D. ISAKMP

ISAKMP *Policy* digunakan sebagai parameter untuk menghubungkan antara R1 dengan R3 untuk membentuk sebuah jaringan Tunnel VPN (TABEL II). R1 dan R3 harus mengunakan Key, Algoritma Enkripsi, Auntentifikasi serta Kode Keamanan ISAKMP yang sama untuk membentuk tunnel VPN. Terlihat pada Tabel 2 merupakan parameter yang digunakan oleh kedua router. R1 dan R3 menggunakan model keamanan ISAKMP dengan menggunakan algritma enkripsi AES 256 dan menggunakan metode auntentifikasi *pre-share* serta menggunakan sandi ISAMKP vpnfmy.

TABEL II
PARAMETER

Parameter		R1	R3
Key Distribute Methode	Manual or ISAKMP	ISAKMP	ISAKMP
Encryption Algorithm	DES, 3 DES, or AES	AES 256	AES 256
Hash Algorithm	MD5 or SHA-1	SHA-1	SHA-1
Authentication Method	Pre-shared keys or RSA	Pre-share	Pre-share
Key Exchange	DH Group 1,2 or 5	DH 5	DH 5
ISAKMP Key		Vpnfmy	Vpnfmy

Untuk melakukan pengimplementasian ISAKMP dan IPSec terdapat beberapa hal yang harus diperhatikan, khususnya parameter pada ISAKMP *Policy*. Terdapat beberapa langkah yang digunakan dalam melakukan pengimplementasian ISAKMP:

```
R1(config)#crypto isakmp policy 10
R1(config-isakmp)# encryption aes 256
R1(config-isakmp)# authentication pre-share
R1(config-isakmp)# group 5
R1(config-isakmp)# exit
R1(config)# crypto isakmp key vpnfmy address
  202.168.20.2

R3(config)# crypto isakmp policy 10
R3(config-isakmp)# encryption aes 256
R3(config-isakmp)# authentication pre-share
R3(config-isakmp)# group 5
R3(config-isakmp)# exit
R3(config)# crypto isakmp key vpnfmy address
  202.168.10.2
```

Langkah pertama yang dilakukan adalah pengimplementasian ISAKMP terhadap R1 dan R3, tunnel yang digunakan diantara kedua router tersebut menggunakan group 5 dengan menggunakan key vpnfmy. Setelah melakukan konfigurasi ISAKMP selanjutnya melakukan konfigurasi IPSec terhadap R1 dan R3.

```
R1(config)# crypto map VPN-MAP 10 ipsec-
  isakmp
R1(config-crypto-map)# description VPN
  connection to R3
R1(config-crypto-map)# set peer 202.168.20.2
R1(config-crypto-map)# set transform-set VPN-
  SET
R1(config-crypto-map)# match address 110
R1(config-crypto-map)# exit

R3(config)# crypto map VPN-MAP 10 ipsec-
  isakmp
R3(config-crypto-map)# description VPN
  connection to R1
R3(config-crypto-map)# set peer 202.168.10.2
R3(config-crypto-map)# set transform-set VPN-
  SET
R3(config-crypto-map)# match address 110
R3(config-crypto-map)# exit
```

E. Uji Konektifitas Skenario 1

Uji konektifitas yang pertama kali dilakukan adalah melakukan pengujian terhadap kinerja jaringan dengan melakukan perbandingan antara jaringan yang menggunakan Tunnel dengan jaringan yang tidak menggunakan tunnel. Pengujian Tunnel VPN dilakukan pada jaringan lokal R1 menuju jaringan lokal R3 khususnya dengan network 192.168.4.0/24. Pengujian VPN Tunnel dapat dilakukan menggunakan perintah ping untuk melakukan pengiriman paket ICMP dan mendapatkan hasil traceroute seperti terlihat pada Tabel 3. Semakin sedikit jumlah hops yang dilalui maka semakin besar pula nilai *Time to Live* (TTL) yang didapatkan. TTL yang didapatkan pada jaringan Tunnel VPN sebesar 126, sedangkan TTL pada jaringan tanpa menggunakan Tunnel sebesar 124.

TABEL III
TRACERT TUNNEL VPN

Source Address	Destination Address	Hops Count
192.168.1.2	192.168.4.2	192.168.1.1 202.168.20.2 192.168.4.2
192.168.2.2	192.168.4.2	192.168.2.1 202.168.20.2 192.168.4.2
192.168.4.2	192.168.1.2	192.168.4.1 202.168.10.2 192.168.1.2
192.168.4.2	192.168.2.2	192.168.4.1 202.168.10.2 192.168.2.2

Dapat dijelaskan dari TABEL III merupakan hasil dari pengujian Tunnel VPN. Hasil yang didapat setelah pengimplementasian Tunnel VPN mampu mengurangi jumlah hops yang dilalui antara R1 menuju R3. Source Address yang berasal dari R1 mampu melakukan pemintasan hops menuju R3 hanya dengan menggunakan hops 202.168.20.2.

F. Uji Konektifitas Skenario 2

Pada Uji konektifitas kedua, penulis mencoba melakukan tracert antara jaringan lokal R1 menuju jaringan lokal R3. Pengujian ini bertujuan untuk mendapatkan hops yang dilalui saat melakukan transfer paket data tanpa adanya Tunnel VPN (Tabel 4).

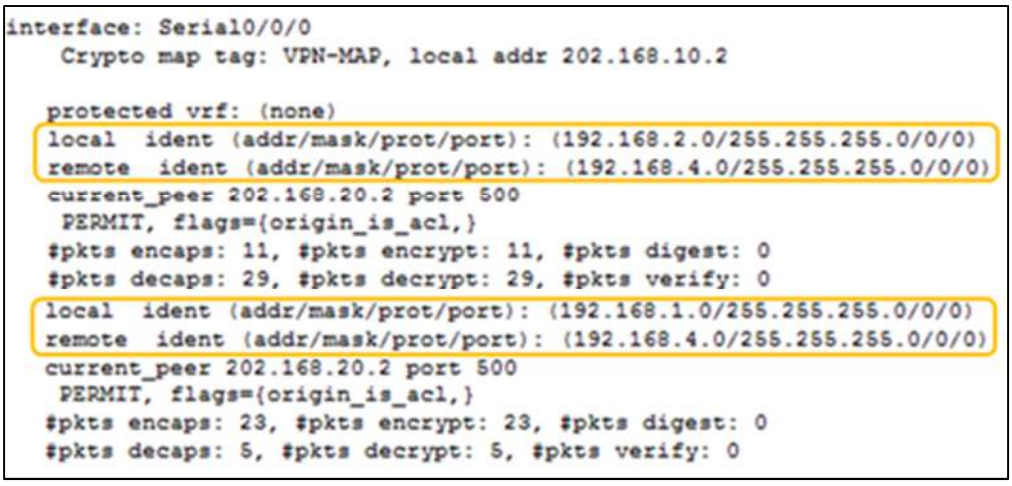
Terlihat pada Tabel 4, jumlah hops yang dilalui saat melakukan transfer data antara network 192.168.1.0/24 menuju 192.168.5.0/24 memiliki 5 (lima) hops. Sedangkan network yang menggunakan Tunnel VPN dengan menggunakan router yang sama mampu melewati hanya sebanyak 3 (tiga) hops saja.

G. Uji Konektifitas Skenario 3

Skenario pengujian yang ketiga adalah melakukan verifikasi terhadap lalu lintas paket data untuk mengetahui paket data tersebut apakah sudah terenkripsi ataupun belum (Gambar 7).

TABEL IV
TRACERT TANPA TUNNEL VPN

Source Address	Destination Address	Hops Count
192.168.1.2	192.168.5.2	192.168.1.1 202.168.10.1 202.168.15.2 202.168.20.2 192.168.5.2
192.168.2.2	192.168.5.2	192.168.2.1 202.168.10.1 202.168.15.2 202.168.20.2 192.168.5.2
192.168.5.2	192.168.1.2	192.168.5.1 202.168.20.1 202.168.15.1 202.168.20.2 192.168.1.2
192.168.5.2	192.168.2.2	192.168.5.1 202.168.20.1 202.168.15.1 202.168.10.2 192.168.2.2



Gambar 7. IPSec Tunnel VPN

Terlihat pada Gambar 7 merupakan hasil uji konektifitas terhadap jaringan IPSec Tunnel VPN. R1 menggunakan interface serial0/0/0 dengan alokasi IP Address 202.168.10.2 untuk dapat melakukan remote terhadap network 192.168.4.0/24. Terdapat dua (2) network yang dapat melakukan Tunnel didalam R1 yaitu network 192.168.2.0/24 menuju 192.168.4.0/24 dan network 192.168.1.0/24 menuju 192.168.4.0/24.

Penggunaan IPSec Tunnel VPN mampu melakukan pengenkripsian terhadap paket data yang dilaluinya. Terlihat pada gambar 6 network 192.168.2.0 melakukan pengiriman paket data menuju network 192.168.4.0/24 sebanyak 11 paket yang telah terenkripsi. Jumlah paket yang terenkripsi akan bertambah secara otomatis ketika terdapat transfer paket data didalam jaringan yang menggunakan Tunnel VPN.

IV. PENUTUP

Simpulan dari penelitian ini adalah bahwa penggunaan Site to Site VPN mampu meminimalisir penggunaan bandwidth pada jaringan internet. Pengimplementasian IPSec dan Enkripsi ISAKMP mampu menjaga keaslian terhadap paket data saat terjadi transfer paket data. Selain itu, pengimplementasian Tunnel VPN mampu meminimalisir terjadinya kebocoran paket data dan Site to Site VPN mampu meringkas hops yang dilalui didalam jaringan internet dengan menggunakan TTL 126.

DAFTAR PUSTAKA

[1] F. A. Salman, "Implementation of IPsec-VPN Tunneling using GNS3," *Indones. J. Electr. Eng. Comput. Sci.*, vol. 7, no. 3, pp. 855–860, 2017.

[2] A. A. Eskandar, M. R. Syed, and M. B. Zarei, "SIP over IP VPN : Performance Analysis," in *Computer Engineering and Applied Computing (WorldComp)*, 2014, vol. 1, no. 1.

[3] I. AFRIANTO and E. B. SETIAWAN, *KAJIAN VIRTUAL PRIVATE NETWORK (VPN) SEBAGAI SISTEM PENGAMANAN (Studi Kasus Jaringan Komputer Unikom)*, vol. 12, no. 1. 2014.

[4] S. R. Ahmed and P. Rajamohan, "Comprehensive performance analysis and special issues of Virtual Private Network strategies in the computer communication: A novel study," *Int. J. Eng. Sci. Technol.*, vol. 3, no. 7, 2013.

[5] D. Tjahjono, R. Shaikh, and W. Ren, "ESTABLISHING AN IPSEC (INTERNET PROTOCOL SECURITY) VPN (VIRTUAL PRIVATE NETWORK) TUNNEL," US 8,893,262 B2, 2014.

[6] R. A. May, "POLICY-BASED CONFIGURATION OF INTERNET PROTOCOL SECURITY FORA VIRTUAL PRIVATE NETWORK," US 9,065,802 B2, 2015.

[7] D. Suprijatmono and D. S. Kartawijaya, "Rancang Bangun Jaringan PABX Berbasis IP Menggunakan Metode IPsec VPN Gateway," *Sainstech*, vol. 28, no. 2, pp. 39–49, 2018.

[8] R. Arlan, R. Munadi, and N. Andini, "IMPLEMENTASI DAN ANALISIS SISTEM KEAMANAN IP SECURITY (IPSEC) DI DALAM MULTI PROTOCOL LABEL SWITCHING-VIRTUAL PRIVATE NETWORK (MPLS-VPN) PADA LAYANAN BERBASIS IP MULTIMEDIA SUBSYSTEM (IMS)," *e-Proceeding Eng.* , vol. 3, no. 3, pp. 4630–4640, 2016.

[9] F. Bensalah, E. Casablanca, and N. EL KAMOUN, "Analytical performance and Evaluation of the Scalability of Layer 3 Tunneling Protocols: Case of Voice Traffic Over IP," *IJCSNS Int. J. Comput. Sci. Netw. Secur.*, vol. 17, no. May, pp. 361–369, 2017.

[10] M. Elezi and B. Raufi, "Conception of Virtual Private Networks using IPsec suite of protocols , comparative analysis of distributed database queries using different IPsec modes of encryption," *Procedia - Soc. Behav. Sci.*, vol. 195, pp. 1938–1948, 2015.

[11] C. Wang and J. Chen, "Implementation of GRE Over IPsec VPN Enterprise Network Based on Cisco Packet Tracer," in *2nd International Conference on Soft Computing in Information Communication Technology*, 2014.

[12] C. Paquet, *Implementasi Cisco IOS Network Security (IINS) Foundation Learning Guide Second Edition*, 2nd ed. USA: Cisco Press, 2013.

[13] A. M. Gamundani and M. Bere, "A VPN Security Solution for Connectivity over Insecure Network Channels : A A VPN Security Solution for Connectivity over Insecure Network Channels : A novel study .," *SSRG Int. J. Comput. Sci. Eng.*, vol. 1, no. October, pp. 1–8, 2014.

[14] G. Aggarwal, P. Shah, A. Thrivikramannair, and D. Blair, "TECHNIQUE FOR USING OER WITH AN ECT SOLUTION FOR MULT-HOMED SITES," US 8,706,883 B2, 2014.

[15] S. Frankel and S. Krishnan, *IP Security (IPsec) and Internet Key Exchange (IKE) Document Roadmap (No. RFC 6071)*. 2011.